REMARKS

Claims 1, 2, 6, 9 and 10 are Allowable

The Office has rejected claims 1, 2, 6, 9 and 10 on page 2 of the Office Action, under 35 U.S.C. §102(b), as being anticipated by U.S. Publication No. 2003/0144952 A1 (Brown et al.). Applicants respectfully traverse the rejections.

None of the cited references, including Brown et al., disclose or suggest the specific combination of claim 1. For example, Brown et al. does not disclose a method comprising providing a notification message to a payment card holder of an attempted transaction using a payment card whether the attempted transaction satisfies a threshold-based rule to allow the notification message to be provided, as recited in claim 1. Support for this claim amendment may be found in at least paragraph [0032] of Applicants' application.

Brown et al. is directed towards an account authorization system for protecting against the fraudulent use of debit and credit cards that can immediately alert the authorities of a crime in progress without tipping off the perpetrator of the crime. *Brown et al.*, paragraphs [0007] and [0008]. The system in Brown et al. features the use of duress PIN numbers that can be input by an account holder – instead of a normal PIN number – in order to alert the authorities without alerting the perpetrator that notification has been given. *Brown et al.*, paragraph [0023]. An account transaction is evaluated through the use of an authorization server that determines whether a PIN number was included in the vendor request. *Brown et al.*, paragraph [0044]. If a PIN number is not included, the account holder is contacted to provide a PIN number. *Brown et al.*, paragraph [0044]. The system determines if the PIN number is normal, and if so the account holder is provided with details of the transaction and is requested to approve or reject the transaction. *Brown et al.*, paragraph [0045]. If the PIN number is the duress PIN number, the authorization server contacts the relevant authorities and provides information on the pending transaction to the account holder so as to appear to the perpetrator that no authorities have been contacted. *Brown et al.*, paragraph [0047].

In contrast to claim 1, Brown et al. does not disclose a method comprising providing a notification message to a payment card holder of an attempted transaction using a payment card whether the attempted transaction satisfies a threshold-based rule to allow the notification message to be provided. In Brown et al., notifications are automatically sent to the account holder regardless of whether a PIN number is or is not provided. Further, it would not have been obvious for one having ordinary skill in the art to modify the system of Brown et al. to include a method comprising providing a notification message to a payment card holder of an attempted transaction using a payment card whether the attempted transaction satisfies a threshold-based rule to allow the notification message to be provided. An objective of Brown et al. is to provide a system to detect unauthorized use of an account when under duress. *Brown et al.*, paragraph [0019]. If situations arose in which attempted transactions were not notified to the account holder when under duress, duress PIN numbers would never be input and hence the authorities would not be notified. As such, modification of Brown et al. to achieve the elements in claim 1 would frustrate the intended purpose of Brown et al. and would not have been obvious. Hence, claim 1 is allowable.

Claims 2, 6, 9 and 10 depend from claim 1, which Applicants have shown to be allowable. Hence, Brown et al. fails to disclose at least one element of each of claims 2, 6, 9 and 10. Accordingly, claims 2, 6, 9 and 10 are also allowable, at least by virtue of their dependency from claim 1.

Further, the dependent claims include additional features that are not disclosed or suggested by Brown et al. For example, claim 10 recites a method wherein the notification message indicates at least part of a number of the payment card. The Office Action states that such a notification message is found in paragraph [0037] of Brown et al. *Office Action*, page 3. The aforementioned portion of Brown et al. discloses informing the account holder of information that may contain the name and address of a vendor, the dollar amount of a transaction, the number of transactions authorized that day, and the dollar amount of transactions authorized that day. *Brown et al.*, paragraph [0037]. However, Brown et al. fails to disclose a method wherein the notification message indicates at least part of a number of the payment card, as recited in claim 10. For this additional reason, claim 10 is allowable.

Claims 11, 12, 16, 19 and 20 are Allowable

The Office has rejected claims 11, 12, 16, 19 and 20 on page 2 of the Office Action, under 35 U.S.C. §102(b), as being anticipated by Brown et al. Applicants respectfully traverse the rejections.

None of the cited references, including Brown et al., disclose or suggest the specific combination of claim 11. For example, Brown et al. does not disclose a system wherein a threshold-based rule is applied by the payment card transaction notification and authorization system to determine whether the notification message is to be provided to the payment card holder, as recited in claim 11. Support for this claim amendment may be found in at least paragraph [0032] of Applicants' application.

Brown et al. is directed towards an account authorization system for protecting against the fraudulent use of debit and credit cards that can immediately alert the authorities of the crime in progress without tipping off the perpetrator of the crime. *Brown et al.*, paragraphs [0007] and [0008]. The system in Brown et al. features the use of duress PIN numbers that can be input by an account holder – instead of a normal PIN number – in order to alert the authorities without alerting the perpetrator of the fact that notification has been given. *Brown et al.*, paragraph [0023]. An account transaction is evaluated through the use of an authorization server that determines whether a PIN number was included in the vendor request. *Brown et al.*, paragraph [0044]. If a PIN number is not included, the account holder is contacted to provide a PIN number. *Brown et al.*, paragraph [0044]. The system determines if the PIN number is normal, and if so the account holder is provided with details of the transaction and is requested to approve or reject the transaction. *Brown et al.*, paragraph [0045]. If the PIN number is the duress PIN number, the authorization server contacts the relevant authorities and provides information on the pending transaction to the account holder so as to appear to the perpetrator that no authorities have been contacted. *Brown et al.*, paragraph [0047].

In contrast to claim 11, Brown et al. does not disclose a system wherein a threshold-based rule is applied by the payment card transaction notification and authorization system to determine whether the notification message is to be provided to the payment card holder. In

Brown et al., notifications are automatically sent to the account holder regardless of whether a PIN number is or is not provided and regardless of any property associated with the transaction. Further, it would not have been obvious for one having ordinary skill in the art to modify the system of Brown et al. to include a system wherein a threshold-based rule is applied by the payment card transaction notification and authorization system to determine whether the notification message is to be provided to the payment card holder. Brown et al. provides a system to detect unauthorized use of an account when under duress. *Brown et al.*, paragraph [0019]. If situations arose in which attempted transactions were not notified to the account holder when under duress, duress PIN numbers would never be input and hence the authorities would never be notified. As such, modification of Brown et al. to achieve the system set forth in claim 11 would frustrate the intended purpose of the Brown et al. reference and would not have been obvious. Hence, claim 11 is allowable.

Claims 12, 16, 19 and 20 depend from claim 11, which Applicants have shown to be allowable. Hence, Brown et al. fails to disclose at least one element of each of claims 12, 16, 19 and 20. Accordingly, claims 12, 16, 19 and 20 are also allowable, at least by virtue of their dependency from claim 11.

Further, the dependent claims include additional features that are not disclosed or suggested by Brown et al. For example, claim 20 recites a system wherein the notification message indicates at least part of a number of the payment card. The Office Action states that such a notification message is found in paragraph [0037] of Brown et al. *Office Action*, page 3. The aforementioned portion of Brown et al. discloses informing the account holder of information that may contain the name and address of the vendor, the dollar amount of the transaction, the number of transactions authorized that day, and the dollar amount of transactions authorized that day. *Brown et al.*, paragraph [0037]. However, Brown et al. fails to disclose a system wherein the notification message indicates at least part of a number of the payment card, as recited in claim 20. For this additional reason, claim 20 is allowable.

Claims 3 and 13 are Allowable

The Office has rejected claims 3 and 13 on page 5 of the Office Action, under 35 U.S.C. §103(a), as being unpatentable over Brown et al. in view of United States Patent No. 5,999,596 (Walker et al.). Applicants respectfully traverse the rejections.

Claims 3 and 13 depend from claims 1 and 11, respectively, which Applicants have shown to be allowable. Walker et al. does not disclose or suggest the elements recited in claims 1 and 11 that are not disclosed or suggested by Brown et al. For example, Walker et al. does not disclose or suggest a method comprising providing a notification message to a payment card holder of an attempted transaction using a payment card whether the attempted transaction satisfies a threshold-based rule to allow the notification message to be provided, as recited in claim 1. Further, Walker et al. does not disclose or suggest a system wherein a threshold-based rule is applied by the payment card transaction notification and authorization system to determine whether the notification message is to be provided to the payment card holder, as recited in claim 11. Thus, claims 3 and 13 are allowable, at least by virtue of their dependency from claim 1 or 11.

Further, claims 3 and 13 include additional features that are not disclosed or suggested by Walker et al. For example, claims 3 and 13 recite providing a message to return the payment card to an individual attempting the transaction. The Office Action states that this feature is disclosed in column 10, lines 45-54 of Walker et al. *Office Action*, page 5. The aforementioned portion of Walker et al. discloses a communication of the account holder who has a parental relationship with the user so that the nature of the emergency can be discerned. *Walker et al.*, column 10, lines 45-55. However, Walker et al. fails to disclose providing a message to return the payment card to an individual attempting the transaction, as recited in claims 3 and 13. For this additional reason, claims 3 and 13 are allowable.

Claims 4 and 14 are Allowable

The Office has rejected claims 4 and 14 on page 5 of the Office Action, under 35 U.S.C. §103(a), as being unpatentable over Brown et al. in view of United States Patent No. 4,114,027 (Slater et al.). Applicants respectfully traverse the rejections.

Claims 4 and 14 depend from claims 1 and 11, respectively, which Applicants have shown to be allowable. Slater et al. does not disclose or suggest the elements recited in claims 1 and 11 that are not disclosed or suggested by Brown et al. For example, Slater et al. does not disclose or suggest a method comprising providing a notification message to a payment card holder of an attempted transaction using a payment card whether the attempted transaction satisfies a threshold-based rule to allow the notification message to be provided, as recited in claim 1. Further, Slater et al. does not disclose or suggest a system wherein a threshold-based rule is applied by the payment card transaction notification and authorization system to determine whether the notification message is to be provided to the payment card holder, as recited in claim 11. Thus, claims 4 and 14 are allowable, at least by virtue of their dependency from claim 1 or 11.

Claims 5, 15, and 22 are Allowable

The Office has rejected claims 5, 15, and 22 on page 6 of the Office Action, under 35 U.S.C. §103(a), as being unpatentable over Brown et al. in view of United States Patent No. 5,819,226 (Gopinathan et al.). Applicants respectfully traverse the rejections.

Claims 5 and 15 depend from claims 1 and 11, respectively, which Applicants have shown to be allowable. Gopinathan et al. does not disclose or suggest the elements recited in claims 1 and 11 that are not disclosed or suggested by Brown et al. For example, Gopinathan et al. does not disclose or suggest a method comprising providing a notification message to a payment card holder of an attempted transaction using a payment card whether the attempted transaction satisfies a threshold-based rule to allow the notification message to be provided, as recited in claim 1. Further, Gopinathan et al. does not disclose or suggest a system wherein a threshold-based rule is applied by the payment card transaction notification and authorization system to determine whether the notification message is to be provided to the payment card holder, as recited in claim 11. Thus, claims 5 and 15 are allowable, at least by virtue of their dependency from claim 1 or 11.

None of the cited references, including Brown et al. and Gopinathan et al. disclose or suggest the specific combination of claim 22. For example, Brown et al. and Gopinathan et al. do not disclose a method wherein the notification message is provided whether the attempted transaction satisfies a threshold-based rule, as recited in claim 22. Support for this claim amendment may be found in at least paragraph [0032] of Applicants' application.

In Brown et al., an account transaction is evaluated through the use of an authorization server that determines whether a PIN number was included in the vendor request. *Brown et al.*, paragraph [0044]. If a PIN number is not included, the account holder is contacted to provide a PIN number. *Brown et al.*, paragraph [0044]. The system determines if the PIN number is normal, and if so the account holder is provided with details of the transaction and is requested to approve or reject the transaction. *Brown et al.*, paragraph [0045]. If the PIN number is the duress PIN number, the authorization server contacts the relevant authorities and provides information on the pending transaction to the account holder so as to appear to the perpetrator that no authorities have been contacted. *Brown et al.*, paragraph [0047].

Gopinathan et al. is directed towards an automated system for detecting fraudulent transactions using a neural network. *Gopinathan et al.*, Abstract. The method uses predictive modeling to perform pattern recognition and classification in order to isolate transactions that have a high probability of fraud. *Gopinathan et al.*, column 1, lines 15-19.

In contrast to claim 22, Brown et al. does not disclose a method wherein the notification message is provided whether the attempted transaction satisfies a threshold-based rule. In Brown et al., notifications are automatically sent to the account holder regardless of whether a PIN number is or is not provided and regardless of any property associated with the transaction. Gopinathan et al. does not disclose providing a notification message to a payment card holder and fails to disclose a method wherein the notification message is provided whether the attempted transaction satisfies a threshold-based rule. The fraud detection scheme in Gopinathan et al. is automated and is specifically designed for instances in which the user is not aware of fraudulent use. *Gopinathan et al.*, column 1, lines 35-36. Further, it would not have been obvious for one having ordinary skill in the art to modify the combination of Brown et al. and Gopinathan et al. to include a method wherein the notification message is provided whether the

attempted transaction satisfies a threshold-based rule. Brown et al. provides a system to detect unauthorized use of an account when under duress. *Brown et al.*, paragraph [0019]. If situations arose in which attempted transactions were not notified to the account holder when under duress, duress PIN numbers would never be input and hence the authorities would never be notified. Modification of Gopinathan et al. to achieve the method of claim 22 would also not have been obvious because Gopinathan et al. is directed towards a system in which all transactions are monitored for fraud without notification or input from the account holder. As such, modification of the combination of Brown et al. and Gopinathan et al. to achieve the method set forth in claim 22 would frustrate the intended purposes of the references and would not have been obvious. Hence, claim 22 is allowable.

Further, it would not have been obvious for one having ordinary skill in the art to combine Brown et al. and Gopinathan et al. in the manner suggest in the Office Action since there is no motivation present to make the asserted combination. Brown et al. is directed towards a system in which a duress PIN number is input and the transaction proceeds as normal so as to alert the authorities yet not tip off the perpetrator. *Brown et al.*, paragraph [0047]. If one were to incorporate the locking of the account feature of Gopinathan et al. into Brown et al., the principle of operation of Brown et al. would be frustrated. For example, if the duress PIN number were entered, and the account holder's account was locked, the perpetrator would become aware that the authorities had been contacted and could potentially harm the account holder in anger or flee the scene to escape capture. Brown et al. seeks to allow transactions to be made while informing the authorities without alerting the perpetrator so that the account holder is not harmed and so that the location of the perpetrator can be tracked. The combination of Brown et al. and Gopinathan et al. in the manner suggested in the Office Action would result in a method that would not work for its intended purpose and, as such, sufficient motivation does not exist for such combination. Therefore, for this additional reason, claims 5, 15 and 22 are allowable.

Claims 7 and 17 are Allowable

The Office has rejected claims 7 and 17 on page 6 of the Office Action, under 35 U.S.C. §103(a), as being unpatentable over Brown et al. in view of United States Patent No. 6,052,675 (Checchio). Applicants respectfully traverse the rejections.

Claims 7 and 17 depend from claims 1 and 11, which Applicants have shown to be allowable. Checchio does not disclose or suggest the elements recited in claims 1 and 11 that are not disclosed or suggested by Brown et al. For example, Checchio does not disclose or suggest a method comprising providing a notification message to a payment card holder of an attempted transaction using a payment card whether the attempted transaction satisfies a threshold-based rule to allow the notification message to be provided, as recited in claim 1. Further, Checchio does not disclose or suggest a system wherein a threshold-based rule is applied by the payment card transaction notification and authorization system to determine whether the notification message is to be provided to the payment card holder, as recited in claim 11. Thus, claims 7 and 17 are allowable, at least by virtue of their dependency from claim 1 or 11.

Further, claims 7 and 17 include additional features that are not disclosed or suggested by Brown et al. and Checchio. For example, the Office Action acknowledges that Brown et al. does not disclose or suggest automatically reporting a fraudulent transaction to a credit reporting agency, as recited in claims 7 and 17. *Office Action*, page 7. Checchio also does not disclose or suggest this feature. Cheechio discloses a method in which a vendor compares the signature on the back of the credit card to the customer's signature. *Checchio*, column 1, lines 22-26. If the signatures do not match the transaction is refused and the police and the credit card company are notified. *Checchio*, column 1, lines 25-30. Notification of the credit card company is not automatically reporting a fraudulent transaction to a credit reporting agency. For this additional reason, claims 7 and 17 are allowable.

Claims 8 and 18 are Allowable

The Office has rejected claims 8 and 18 on page 7 of the Office Action, under 35 U.S.C. §103(a), as being unpatentable over Brown et al. in view of United States Publication No. 2003/0182214 A1 (Taylor). Applicants respectfully traverse the rejections.

Claims 8 and 18 depend from claims 1 and 11, respectively, which Applicants have shown to be allowable. Taylor does not disclose or suggest the elements recited in claims 1 and 11 that are not disclosed or suggested by Brown et al. For example, Taylor does not disclose or suggest a method comprising providing a notification message to a payment card holder of an

attempted transaction using a payment card whether the attempted transaction satisfies a threshold-based rule to allow the notification message to be provided, as recited in claim 1. Further, Taylor does not disclose or suggest a system that a threshold-based rule is applied by the payment card transaction notification and authorization system to determine whether the notification message is to be provided to the payment card holder, as recited in claim 11. Thus, claims 8 and 18 are allowable, at least by virtue of their dependency from claim 1 or 11.

Further, claims 8 and 18 include additional features that are not disclosed or suggested by Brown et al. and Taylor. For example, the Office Action acknowledges that Brown et al. does not disclose or suggest sending a reason code to a merchant, as recited in claims 8 and 18. *Office Action*, page 7. Taylor also does not disclose or suggest sending a reason code to a merchant. Taylor discloses sending a response code to a bank teller. *Taylor*, paragraph [0044]. A bank teller is not a merchant. For this additional reason, claims 8 and 18 are allowable.

Claim 21 is Allowable

The Office has rejected claim 21 on page 8 of the Office Action, under 35 U.S.C. §103(a), as being unpatentable over Brown et al. in view of United States Publication No. 2003/0014367 (Tubinis). Applicants respectfully traverse the rejection.

Claim 21 depends from claim 11, which Applicants have shown to be allowable. Tubinis does not disclose or suggest the elements recited in claim 11 that are not disclosed or suggested by Brown et al. For example, Tubinis does not disclose or suggest a system wherein a threshold-based rule is applied by the payment card transaction notification and authorization system to determine whether the notification message is to be provided to the payment card holder, as recited in claim 11. Thus, claim 21 is allowable, at least by virtue of its dependency from claim 11.

CONCLUSION

Applicants have pointed out specific features of the claims not disclosed, suggested, or rendered obvious by the references applied in the Office Action. Accordingly, Applicants

respectfully requests reconsideration and withdrawal of each of the objections and rejections, as well as an indication of the allowability of each of the pending claims.

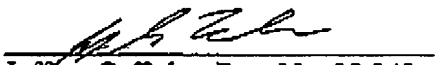
Any changes to the claims in this response, which have not been specifically noted to overcome a rejection based upon the prior art, should be considered to have been made for a purpose unrelated to patentability, and no estoppel should be deemed to attach thereto.

The Examiner is invited to contact the undersigned attorney at the telephone number listed below if such a call would in any way facilitate allowance of this application.

The Commissioner is hereby authorized to charge any fees, which may be required, or credit any overpayment, to Deposit Account Number 50-2469.

Respectfully submitted,

11-9-2007
Date



Jeffrey G. Toler, Reg. No. 38,342
Attorney for Applicant(s)
TOLER SCHAFFER LLP
8500 Bluffstone Cove, Suite A201
Austin, Texas 78759
(512) 327-5515 (phone)
(512) 327-5575 (fax)